Cyber Threat Intelligence

Insights

Cyber-Weather

December

From January 1, 2022, Capgemini is bringing together its cybersecurity forces, originating from Sogeti and Capgemini Cloud Infrastructure Services, into a single entity, which operates under the Capgemini brand.

Cyber-Weather
Anticipation

Weak signals for Strategic CTI

Log4j : chronicles of an IT disaster

On November 24, 2021, Alibaba Cloud security research team officially submitted a vulnerability to Apache, which will then be tracked under the tag #CVE-2021-44228.
This vulnerability, dubbed "#Log4Shell" uses a weakness in #Apache #Log4j2, a Java-based logging tool that is widely used in all Java-based developments to track all information about Java items in the form of event logs. **This #RCE is considered as highly critical as #Java is used in billions of applications globally, mostly with #Log4j2 tool available**. Following the tremendous reactivity of #Apache teams (which is a non-profit charity, it's important to highlight that), the version 2.15 were published. **But the patch didn't correct all malicious exploitations possibilities so a new vulnerability that could lead to a limited** #RCE **tracked as #CVE-2021-45046 were addressed in version 2.16**. The nightmare continued with the Apache's statement regarding that this version doesn't protect from uncontrolled recursion from self-referential lookups in Log4j. **This flaw can be exploited via the #CVE-2021-45105 and can lead to a #DoS so the version 2.17.1 was published**. This is the updated version as of writing.

The ease of exploitation of the vulnerability and the massive presence of Log4j in information systems around the world represent a boon for malicious actors. **Within hours of the PoC release, massive scans were detected looking for vulnerable applications and services.** The first (at our best knowledge as of writing) to exploit #Log4Shell were mostly #botnets (Mirai & Tsunami) and #cryptominers (XMrig). **But more sophisticated adversaries rapidly followed** and first #eCrime and #RaaS actors were spotted (Wizard Spider with Conti for example or Evil Corp with Dridex) along their favorite tools (Cobalt Strike). **The most worrying is probably the rapid exploitation of the flaw by state-sponsored actors** such as #APT35 (Iran), #Hafnium (China) and unnamed Turkish but also North-Korea ones.

The fact that Wizard Spider is interested by Log4j is very worrying due to its sophistication and its toolset. It's clearly a privateer group that weak signals bring us to link them with medium confidence to Moscow efforts to disturb Occidental countries economic and political tissues. As the cartelization of the #eCrime sphere is a hot topic since few months, **it's highly likely that other cartels of other ransomware developers such the one led by Lockbit enters the game to monetize #Log4Shell flaws in a Big Game Hunting effort**.
If the #APT35 implication seems, as usual, to be directed to regional rivals of Tehran (i.e Israel), the #Hafnium operations are historically global and aim to target large networks of large companies without targets discrimination. #Hafnium has already exploited the ProxyLogon flaws on Microsoft Exchange servers so **they seem to specialize themselves in exploiting fresh and juicy CVEs as Log4j is**. It's pretty sure that #Hafnium leverages #Log4Shell to perform cyber espionage operations gaining quiet and persistent foothold on targets of interest for China. For now, **Russian APT groups have not been spotted : it's probably a matter of time knowing their activism when this kind of flaw becomes public.**

- **Focus efforts** on patches published by Apache teams that are reflected in the CTI Flash News regularly updated
- You can **identify vulnerables applications launching scans** promoted by the CTI Team in our Flash News such as the CISA one dubbed Log4jScanner.
- Regularly **test your backups & maintain them offline**
- **Pay attention to all detections based on IoCs provided by the CTI Team linked to Log4Shell** : they could be noisy but an ounce of prevention is worth a pound of cure.
- **Regularly check the** Apache page to get insights about potential new CVEs or new mitigations posted about Log4j

CVE-2021-44228, Log4Shell, Log4J2, Apache, RCE, Java, CVE-2021-45046, CVE-2021-45105, DoS, Botnets, Cryptominers, eCrime, RaaS, APT35, Hafnium

#

## APT

### APT27 (aka Emissary Panda, Lucky Mouse)

People's Republic of China

- Asia & Middle East
- Global sometimes

- Polar Ransomware
- ProxyLogon exploitation
- Strategic web compromises
- SysUpdate
- PlugX & ShadowPad

#APT27 (aka #Emissary Panda, #Lucky Mouse) is a **Chinese APT group believed to operate on behalf of the People's Republic of China (PRC)**.

#APT27 usually targets **Central Asia countries and Middle-East ones but it can also expand its targeting to Occidental entities**. Recent campaigns of Emissary Panda seem to follow the Chinese agenda of the Belt and Road Initiative targeting countries involved in this project .

Active since 2010, #APT27 **heavily relies on strategic web compromises to target victims**. Among its toolset, it's not surprising to see this group using several tools shared by numerous Chinese APT groups such as the #PlugX backdoor, #beEF, or #ShadowPad C2 infrastructure (aka Axiomatic asymptote). What it's noteworthy is the use by the group of the #Polar ransomware on May 2020. **This incident could indicate that APT27 is involved both in cyberespionage operations but also in financially motivated ones as other APT groups such as Lazarus or Winnti (aka #APT41).**

The FBI recently published an advisory about **active exploitation of the Zoho's Manage Engine via the CVE-2021-44515** : Manage Engine installations were already targeted between August and October 2021 by a threat group that TTPs overlap with #APT27 ones.

REDACTED COMMENT AVAILABLE ON PRIVATE VERSION

# APT27, Emissary Panda, Lucky Mouse, PlugX, beEF, Shadow Pad, Polar ransomware, ANSSI, APT41

E-crime

Blackcat (aka Noberus, ALPHV)

Commonwealth of Independent States

- Opportunistic
- Big Game Hunting

- Relies on Rust programming language
- Likely uses ScreenConnect as an entry point

#BlackCat is a new ransomware, first reported in the wild on 9 December. Although some malwares have already been written in #Rust, **this is the first ransomware in our best knowledge that uses this language** (which provides higher performance and better security levels than C++). #BlackCat is also a #doxware, meaning that it has a #Tor infrastructure through which it exfiltrates its victims' previously encrypted data in order to undermine their competitiveness and get them to pay the ransom.

Among singular aspects of #ALPHV (alias for #BlackCat), **we can note that some researchers claim that the author of BlackCat could have been one of the now defunct Revil/Sodinokibi RaaS affiliates**. Moreover, each #ALPHV ransomware executable includes a JSON configuration that allows for customization of extensions, ransom notes, how data will be encrypted, excluded folders/files/extensions, and services and processes to be terminated automatically. #BlackCat can also be configured with domain credentials that can be used to spread the ransomware and encrypt other devices on the network. **All these patterns can indicate that #BlackCat could be one of the most sophisticated ransomware strains in the eCrime ecosystem**. And the reason for that is probably the identity of its developers : **some arguments point that #BlackCat may be the last tool of the infamous #FIN7** (aka Carbon Spider) after having shut down DarkSide and #BlackMatter ransomwares.

As of writing, **we're aware of a spike in compromises on our clients partners realized by #BlackCat which is worrying if we study the rhythm of its compromises**.

# BlackCat, Rust, Doxware, ALPHV, FIN7, BlackMatter

Vulnerabilities

CVE-2021-21220

Insufficient validation of untrusted input in V8

Zero Day Initiative Security researcher Hossein Lotfi have demonstrated a proof of concept (POC) code to exploit **CVE-2021-21220.** Due to Insufficient validation of untrusted input in v8 (Javascript engine), the Just In Time (JIT) JavaScript compilation engine used in **Google Chrome** and **Microsoft Edge** can be abused to generate code that produces an incorrect numeric result.

By leveraging two primitives (one to learn the numeric value of an object's address and one to inject arbitrary pointer value) an attacker can override the **wasm** function with a shellcode. Therefore, this heap corruption results into a powerful **Remote Code Execution** (RCE).

This technique is particularly deadly if the vulnerability is exploited by an attacker performing phishing campaigns using a crafted HTML page to gain initial access to a network. Indeed, the victim just need to click a link to be compromised.

Course of action

It is strongly recommended to patch Google Chrome and Microsoft Edge to the latest version.

Vulnerability, Google, Chrome, Windows, Microsoft, Edge, RCE, CVE-2021-21220, JIT

CVE-2021-44790 / CVE-2021-44224

Apache HTTP Server vulnerabilities

Apache addressed two vulnerabilities that could lead to **remote code execution** (RCE).
The vulnerability tracked as **CVE-2021-44790** take advantage of the mod_lua of **Apache HTTP Server** <= 2.4.51 multipart content parser that could lead to a possible **buffer overflow** when called from a Lua script.

An additional flaw tracked as **CVE-2021-44224** allows an attacker to craft a request that once send to https configured as a forwarded proxy can cause a **NULL pointer dereference**. This flaw could also be exploited to allow a **Server-Side Request Forgery** (SSRF). Indeed, a crafted URI could also be used to make reverse proxy declarations and allow requests to be redirected to a remote declared Unix Domain socket.

Our CTI team and the team at Apache did not spot any exploit in the wild at the time of writing of this CyberWeather.

Course of action

It is strongly recommended to patch Apache HTTP Server to the latest version (2.4.52).

Apache, RCE, CVE-2021-44790, CVE-2021-44224, Multipart

Capgemini

Cyber-Weather

Evolution of top-tier ransom-dox-wares

EGREGOR | NETWALKER

#Egregor reduced its activity in **January.** #Netwalker have been been <u>seized</u> the 27th of January by the U.S. Department of Justice

CONTI | PYSA

#Conti had a peak of activity until dividing its rate by 2 since **June** 2021
#Pysa had a peak of activity till **May** 2021

REVIL | AVADDON | DARKSIDE

#Revil had a peak of activity till they claimed responsibility for a hack at the IT firm Kaseya **in July**
#DarkSide has **gone dark** after more than $2 million was <u>seized</u> by the U.S Department of Justice in **June**
#Avaddon has **shut down** operation and released the decryption keys

COOMINGPROJECT | LOCKBIT | CONTI | BLACKMATTER

#LockBit makes a huge progress in September almost doubling its activity while #CoomingProject counts already more than 20 victims and #Conti, #Pysa & #Blackmatter (ex #Darkside) continue at a huge pace

PYSA | ClOP | CUBA | PAYLOAD.BIN | LOCKBIT

#Pysa, #ClOP, #Cuba and Payload.bin in **August**. After one month Lockbit return with a version 2.0

LOCKBIT | PYSA | CONTI | SPOOK

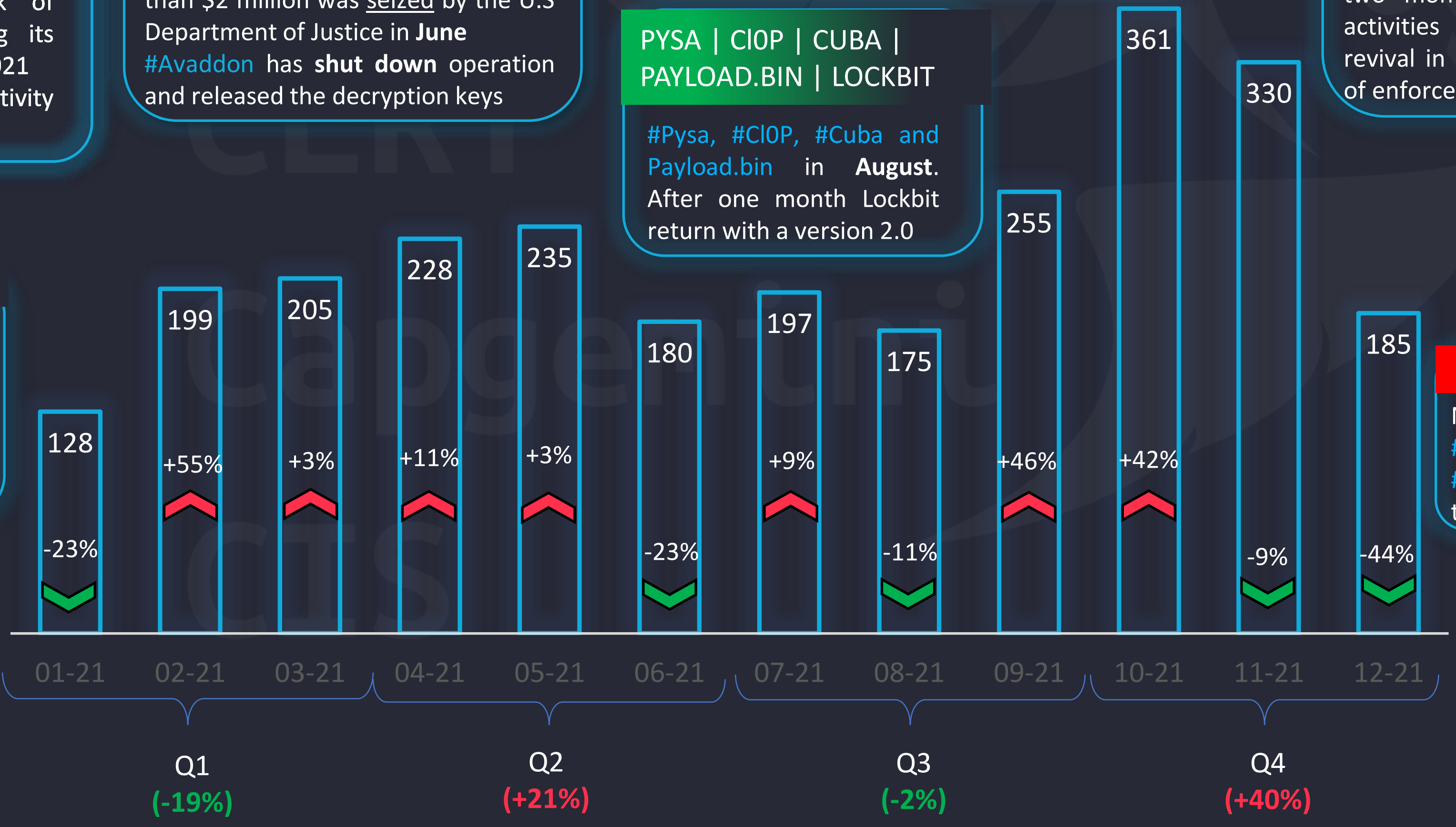
#LockBit is the more active ransomware with almost 100 victims in October where #Conti and #Pysa are behind with about 40~50 victims #Prometheus rebrand as #Spook at the end of Sept and start in October with about 50 victims. After only two months, #Coomingproject stops its activities and #Revil went dark after its revival in September and being the target of enforcement forces

LOCKBIT | PYSA | CONTI | SPOOK

#LockBit and #Conti are leading the board in November with around 90 victims each #Pysa stay behind with 59 victims.

BLACKMATTER | REVIL |SPOOK

No more activities in November from #Spook, #Payload.bin, #Groove, #AtomSilo, #BlackMatter or #REvil the last 2 being targeted by law enforcement forces



Total Number of top-tier ransom-dox-ware victims (2021)

Sources: DarkTracer, DarkFeed, InterCert, CTI | CERT ESEC

Legend

- 🟥 Shutdown/Ceased
- 🟩 Online & active
- 🟨 Online & inactive
- 🟦 New this month